

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2004-023597**

(43)Date of publication of application : **22.01.2004**

(51)Int.Cl. **H04L 12/66**
G06F 15/00

(21)Application number : **2002-178039** (71)Applicant : **ARIEL NETWORKS CO LTD**

(22)Date of filing : **19.06.2002** (72)Inventor : **INOUE SEIICHIRO**
HIDAKA TAKAHIRO
OTANI HIROYOSHI
IWATA SHINICHI

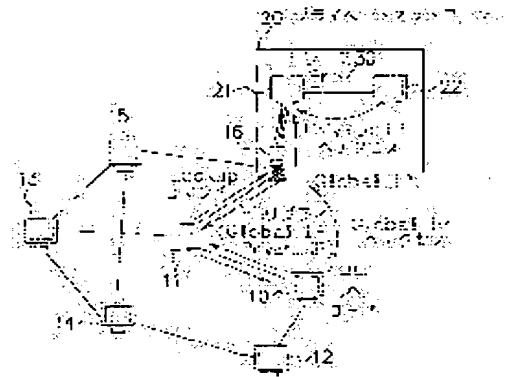
(54) NETWORK SYSTEM AND PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a P2P (peer-to-peer) system that permits externally free access for acquisition of its resource even when the system is installed with a firewall or a NAT (network address translation) server.

SOLUTION: When a gateway node (NAT server) 16 for replacing a global address with a private address receives a hit reply from a node 21 in a private network 20, the node 16 attaches the information of the gateway node 16 to the information of a searching hit node 21 and propagates the added information. When a command issue source node 10 receiving the hit reply cannot establish an access session to the searching hit node 21, the node 10 selects the gateway node 16 in place of the node 21 and executes its access to the node 16 so that the node 10 can freely access the inside of the private network 20 from the outside to acquire a resource 30 even when the NAT server is present in the system.

第2の実施形態によるネットワーク



LEGAL STATUS

[Date of request for examination] **25.05.2005**

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

BEST AVAILABLE COPY

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-23597

(P2004-23597A)

(43) 公開日 平成16年1月22日(2004.1.22)

(51) Int. Cl.⁷H04L 12/66
G06F 15/00

F1

H04L 12/66 B
G06F 15/00 310D

テーマコード(参考)

5B085
5K030

審査請求 未請求 請求項の数 4 O L (全 16 頁)

(21) 出願番号 特願2002-178039 (P2002-178039)
(22) 出願日 平成14年6月19日(2002.6.19)(71) 出願人 502220160
アリエル・ネットワーク株式会社
東京都目黒区中目黒3-3-2 EGビル
7F
(74) 代理人 100105784
弁理士 橋 和之
(72) 発明者 井上 誠一郎
東京都世田谷区野毛2丁目19番8号 グ
リーンハイムA103
(72) 発明者 日高 孝寛
神奈川県川崎市高津区久本3丁目6番12
-208号
(72) 発明者 大谷 弘喜
神奈川県平塚市袖が浜17番47-103
号

最終頁に続く

(54) 【発明の名称】 ネットワークシステムおよびプログラム

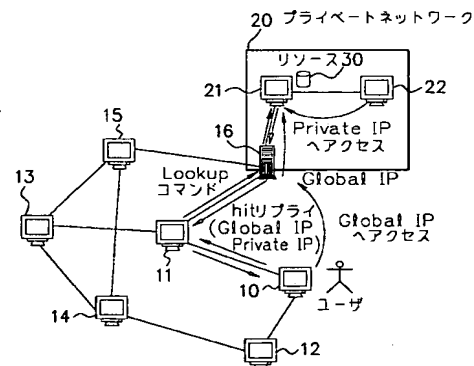
(57) 【要約】

【課題】 ファイアウォールやNATサーバを設置した場合でも、外部から自由にアクセスしてリソースを取得可能なP2Pシステムを提供する。

【解決手段】 グローバルアドレスとプライベートアドレスとの付け替えを行うゲートウェイノード(NATサーバ)16がプライベートネットワーク20内のノード21からhitリプライを受け取ったときに、検索ヒットノード21の情報にゲートウェイノード16の情報を加えて伝播するようにするとともに、hitリプライを受け取ったコマンド発行元ノード10から検索ヒットノード21にアクセスのセッションが張れない場合に、ゲートウェイノード16に切り替えてアクセスを実行するようにすることにより、NATサーバが存在する場合でも、プライベートネットワーク20の外部から内部へと自由にアクセスしてリソース30を取得することができるようにする。

【選択図】 図1

第1の実施形態によるネットワーク



【特許請求の範囲】

【請求項 1】

接続している近接ノード群にリソース検索コマンドを伝播していき、あるノードにおいてリソースの検索にヒットした場合、当該検索ヒットノードから検索ヒット応答を、上記リソース検索コマンドを伝播した各ノードにより逆向きに伝播してコマンド発行元ノードまで届けた後、上記コマンド発行元ノードが上記検索ヒットノードにアクセスして上記リソースを取得するように成されたネットワークシステムであって、

グローバルアドレスとプライベートアドレスとの付け替えを行うことによってプライベートネットワークの内外で通信のやり取りを行うゲートウェイノードを有し、当該ゲートウェイノードは、上記検索ヒット応答を受け取ったときに、上記検索ヒットノードの情報に
10
上記ゲートウェイノードの情報を加えて上記検索ヒット応答を他のノードに転送する手段を備え、

各ノードは、自身が上記コマンド発行元ノードである場合に、上記検索ヒット応答中に含まれる上記検索ヒットノードの情報および上記ゲートウェイノードの情報に基づいて、上記検索ヒットノードもしくは上記ゲートウェイノードにアクセスする手段を備えたことを特徴とするネットワークシステム。

【請求項 2】

接続している近接ノード群にリソース検索コマンドを伝播していき、あるノードにおいてリソースの検索にヒットした場合、当該検索ヒットノードから検索ヒット応答を、上記リ
20
ソース検索コマンドを伝播した各ノードにより逆向きに伝播してコマンド発行元ノードまで届けた後、上記コマンド発行元ノードが上記検索ヒットノードにアクセスして上記リソースを取得するように成されたネットワークシステムであって、各ノードは、

自身が上記コマンド発行元ノードである場合において、上記検索ヒットノードにアクセスできないときに、上記接続している近接ノード群にアクセス要求コマンドを発行するアクセス要求手段と、

自身が上記検索ヒットノードである場合において、伝播されてきた上記アクセス要求コマンドを受け取ったときに、上記コマンド発行元ノードにアクセスを実行する逆アクセス手段とを備えたことを特徴とするネットワークシステム。

【請求項 3】

上記各ノードは、自身が上記コマンド発行元ノードである場合において、上記アクセス要求コマンドを発行したにもかかわらず上記検索ヒットノードからのアクセスが確立されな
30
いときに、所定のゲートウェイノードにアクセスする第 1 のゲートウェイアクセス手段と

、
上記ゲートウェイノードへのアクセスを要求するゲートウェイアクセス要求コマンドを上記接続している近接ノード群に発行する第 2 のアクセス要求手段と、自身が上記検索ヒットノードである場合において、伝播されてきた上記ゲートウェイアクセス要求コマンドを受け取ったときに、上記ゲートウェイノードにアクセスする第 2 のゲートウェイアクセス手段とを備えたことを特徴とする請求項 2 に記載のネットワークシステム。

【請求項 4】

請求項 1 ～ 3 の何れか 1 項に記載の各手段としてコンピュータを機能させるためのプログラム。
40

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明はネットワークシステムおよびプログラムに関し、特に、サーバを介さずにクライアント同士で直接データの交換を行うシステムに用いて好適なものである。

【0002】

【従来の技術】

近年、インターネットの浸透とインターネットユーザ数の爆発的増加という社会的背景、
50
パーソナルコンピュータ（パソコン）の高性能化とネットワークの高速化という技術的背

景をもとに、ピアツーピア（P2P）と呼ばれるネットワーク技術が注目を集めている。

【0003】

従来のネットワークシステムは、少数のサーバと多数のクライアントとをネットワークを介して接続したものが殆どであり、クライアントで生成されたリソースはサーバに集められて管理されていた。ところが、爆発的ユーザ数増加の中、ユーザの生み出したリソースをサーバに集めるコストは無視できないものになっている。

【0004】

すなわち、従来のWebアーキテクチャにおいてサーバにリソースを集める際に、インターネット上に散らばっているリソースを発見するメカニズムには、ディレクトリサービスとサーチエンジンの2つのタイプが存在する。前者は人海戦術と呼ぶべきアプローチで、
10 人手の作業によってリソースを集めるものである。後者はエージェントロボットがインターネットを巡回することによってリソースを集めてまわるものであり、何れのタイプも言わば力任せのアプローチである。

【0005】

また、サーバに集められたリソースは、アクセスの集中を生む。この結果、クライアントとして用いられる高性能なパソコンは殆ど遊休状態となり、高速ネットワークもサーバ周辺だけがいびつに混雑する結果となっている。

【0006】

これに対し、P2Pによるネットワーク技術は、ユーザに近い部分でサーバを介さずに、クライアント同士がダイレクトに情報のやり取りをするアーキテクチャである。つまり、
20 多数のクライアントで生成されたリソースはそれぞれのクライアント自身で管理されるため、多数のリソースをサーバに集める必要もないし、リソース取得のためにアクセスの集中が生じることも殆どない。また、高性能なパソコンが持つ遊休資源を有効に使うことも可能となる。

【0007】

図11を参照して、P2Pアーキテクチャを利用して所望のリソースを検索および取得する際の手順を説明する。図11は、P2Pアーキテクチャが適用されるネットワークの概略構成を示す図である。P2Pネットワークは、ノードの集合で定義される。ノードとは、
30 P2Pプロトコルを実装したプログラムのプロセスのことを言う。したがって、例えば1つのパソコンの中にも、起動しているプログラムが複数あれば、複数のノードが存在することになる。

【0008】

ノード同士は、複数のセッションを互いに張った状態でトポロジを形成する。この常態的なセッションを「接続」と呼ぶことにする。「接続」が常態的なトポロジ形成をなして、この接続セッション上を基本的なプロトコル（リソース検索コマンドに相当するlook
upコマンドや、検索ヒット応答に相当するhitリプライ等）が流れる。

【0009】

これに対して、ユーザノード100（look upコマンドの発行元ノード）からリソース110の存在するノード103（hitリプライの発行元ノード）に対して張るセッションを「アクセス」と呼ぶことにする。「アクセス」は、リソース発見後にコマンド発行
40 元ノードと検索ヒットノードとの間に一時的に張られるセッションで、この上をアクセスインタフェースに応じたプロトコルが流れる。

【0010】

上記した「接続」および「アクセス」のトポロジ形成の状態は中央で管理されず、個々のノードが自律的に形成する。まず、図11（a）のように、リソース110の取得を希望しているユーザのノード100は、どこにリソース110があるかを探し出すためのlook
upコマンドを近接ノード（接続しているノード）101、102に発行する。

【0011】

look upコマンド受け取ったノード101、102は、要求されているリソース110を自身が持っているかどうかを調べる。該当するリソース110が見つからない場合は
50

、図11(b)のように、lookupコマンドを近接ノード(lookupコマンドの送信元以外で接続しているノード)103~106に転送する。このlookupコマンドを受け取ったノード103~106も、要求されているリソース110を自身を持っているかどうかを調べる。

【0012】

このようにコマンド伝播とリソース110の検索を繰り返していく中で、ノード103では、リソース110の検索にヒットする。検索にヒットした場合は、図11(c)に示すように、lookupコマンドの送信元であるノード101にhitリプライを返す。hitリプライを受け取ったノード101は、lookupコマンドの送信元であるユーザノード100にhitリプライを転送する。このようにhitリプライは、lookupコマンドを伝播した各ノードにより逆向きに伝播され、コマンド発行元のユーザノード100まで届けられる。

10

【0013】

hitリプライは、リソース110のアクセスインタフェースの名前と検索ヒットノード103の情報とを含むパケットである。以上の手順により、最初にlookupコマンドを発行したユーザノード100では、所望のリソース110がノード103に存在することを発見できる。hitリプライを受け取ったユーザノード100は次に、図11(d)のようにノード103にダイレクトにアクセスし、リソース110を取得する。

【0014】

【発明が解決しようとする課題】

20

上述のようなP2Pアーキテクチャを利用して、種々のネットワークシステムを構築することが期待されている。例えば、P2Pプロトコルをベースにして、個人またはグループのスケジュールやタスクの管理、文書等のファイル管理、プロジェクトの進捗管理などを行うグループウェアなどを構築することが望まれている。

【0015】

しかしながら、上記従来のP2Pネットワーク技術では、ファイアウォールやNAT(Network Address Translation)があると、グループ内向きのセッションが張れず(接続やアクセスができない)、通信上の大きな障害が発生するという問題があった。

【0016】

30

ファイアウォールは、一般的には1台のサーバをグループの出入口に用い、ここで専用のソフトウェアを動作させることによって、アクセス権を持たない第三者がグループ内に不正に侵入するのを防ぐものである。具体的には、送信元と送信先のIPアドレスを見て通信の可否を判断する。したがって、ファイアウォールが設置されていると、グループの外側から内側に向けての通信が拒否され、接続およびアクセスのセッションを張ることができなくなってしまう。

【0017】

また、NATは、IPアドレスの不足に対応するために考え出された手法である。これは、グループの出入口となるゲートウェイにだけグローバルアドレスを割り振り、グループ内部では当該グループ内でのみ通用するプライベートアドレスを割り振ることにより、グローバルアドレスを節約しようとするものである。ゲートウェイとなるNATサーバは、グループ外部から送られてきたグローバルアドレスをプライベートアドレスに変換することにより、グループ内のノードにアクセスする。

40

【0018】

したがって、ゲートウェイとしてNATサーバが設置されている場合、lookupコマンドの発行元ノードがグループの外側にあり、コマンド伝播によって発見されたノードがグループの内側にあると、グローバルアドレスを持つ外部ノードからプライベートアドレスを持つ内部ノードに対して直接アクセスのセッションを張ることができなくなってしまう。

【0019】

50

P2Pアーキテクチャを用いてグループウェアを構築する場合、グループ内のデータが第三者によって不正に盗聴または改ざんされる危険性から守ると同時に、グループのメンバーが外部からもアクセスできるようにすることが望まれる。LANが構築されている社内だけでなく、自宅や外出先からアクセスできるようにすることが好ましいからである。しかし、セキュリティ対策やIPアドレス確保のためにファイアウォールやNATサーバを設置すると、上述のように内向きのセッションが張れなくなり、外部からのアクセスができないという問題があった。

【0020】

本発明は、このような問題を解決するために成されたものであり、ファイアウォールやNATサーバを設置した場合でも、外部から自由にアクセスしてリソースを取得可能なP2Pシステムを提供することを目的とする。

10

【0021】

【課題を解決するための手段】

本発明のネットワークシステムは、グローバルアドレスとプライベートアドレスとの付け替えを行うことによってプライベートネットワークの内外で通信のやり取りを行うゲートウェイノードを有し、当該ゲートウェイノードは、検索ヒット応答を受け取ったときに、検索ヒットノードの情報にゲートウェイノードの情報を加えて検索ヒット応答を他のノードに転送する手段を備え、各ノードは、自身がコマンド発行元ノードである場合に、検索ヒット応答中に含まれる検索ヒットノードの情報およびゲートウェイノードの情報に基づいて、検索ヒットノードもしくはゲートウェイノードにアクセスする手段を備えたことを特徴とする。

20

【0022】

本発明の他の態様では、各ノードが、自身がコマンド発行元ノードである場合において、検索ヒットノードにアクセスできないときに、接続している近接ノード群にアクセス要求コマンドを発行するアクセス要求手段と、自身が検索ヒットノードである場合において、伝播されてきたアクセス要求コマンドを受け取ったときに、コマンド発行元ノードにアクセスを実行する逆アクセス手段とを備えたことを特徴とする。

【0023】

本発明の他の態様では、各ノードが、自身がコマンド発行元ノードである場合において、アクセス要求コマンドを発行したにもかかわらず検索ヒットノードからのアクセスが確立されないときに、所定のゲートウェイノードにアクセスする第1のゲートウェイアクセス手段と、ゲートウェイノードへのアクセスを要求するゲートウェイアクセス要求コマンドを、接続している近接ノード群に発行する第2のアクセス要求手段と、自身が検索ヒットノードである場合において、伝播されてきたゲートウェイアクセス要求コマンドを受け取ったときに、ゲートウェイノードにアクセスする第2のゲートウェイアクセス手段とを備えたことを特徴とする。

30

【0024】

【発明の実施の形態】

（第1の実施形態）

以下、本発明の第1の実施形態を図面に基づいて説明する。

40

図1は、第1の実施形態によるネットワークの概略構成例を示す図である。本実施形態のネットワークは、ノードの集合10～16、21～22を含んで構成されている。

【0025】

図1の例において、ノード21、22によってプライベートネットワーク20が構成されている。したがって、このノード21、22間では、プライベートIPアドレス（以下、プライベートIPと略す）に基づいてアクセスが行われる。一方、ノード10～16は、プライベートネットワーク20の外部に存在するノードである。したがって、これらのノード10～16間では、グローバルIPアドレス（以下、グローバルIPと略す）に基づいてアクセスが行われる。

【0026】

50

ノード16はNATサーバであり、グローバルIPとプライベートIPとの双方を持つ。プライベートネットワーク20の外部からパケットが送られてきたときは、その宛て先グローバルIP（NATサーバ16のグローバルIP）をプライベートIPに変換することにより、プライベートネットワーク20内のノード21にアクセスする。逆に、プライベートネットワーク20内のノード21からパケットが送られてきたときは、その送信元プライベートIP（ノード21のプライベートIP）をNATサーバ16のグローバルIPに変換して外部のノードにアクセスする。

【0027】

本実施形態では、NATサーバ16のポートフォワード機能を利用して、P2Pアーキテクチャ用のポートを転送する設定を行う。すなわち、マスカレードノードとしてNATサーバ16を設定する。これによりNATサーバ16は、hitリプライを転送するときに、リソースの検索にヒットした検索ヒットノードの情報と、マスカレードノードであるNATサーバ16の情報との双方を転送するように処理する。

10

【0028】

例えば、図1のようにlookupコマンドの発行元ノード10がプライベートネットワーク20の外部にあり、所望のリソース30を備えた検索ヒットノード21がプライベートネットワーク20の内部にある場合について考える。この場合においてNATサーバ16は、検索ヒットノード21から送られてきたhitリプライを転送するときに、検索ヒットノード21のプライベートIPに対して、マスカレードノードであるNATサーバ16のグローバルIPを加えて、その両方のノード情報を転送するようにする。

20

【0029】

このhitリプライを受信したコマンド発行元ノード10は、hitリプライ中に含まれている検索ヒットノード21のプライベートIPに基づいて、通常の処理に従って当該検索ヒットノード21にアクセスを試みる。

【0030】

しかし、コマンド発行元ノード10から検索ヒットノード21に対してはアクセスのセッションを直接張ることができない。そこで、コマンド発行元ノード10は、hitリプライ中に含まれているNATサーバ16のグローバルIPに基づいて、マスカレードノードへのアクセスに切り替えて検索ヒットノード21に間接的にアクセスする。

【0031】

図2は、NATサーバ16の動作を示すフローチャートである。このフローチャートは、NATサーバ16が他のノードから何らかのコマンドを受信した際の動作を示すものである。図2において、NATサーバ16は、受信したコマンドがlookupコマンドかどうかを判断し（ステップS1）、そうであればそのlookupコマンドを他のノードに伝播する（ステップS2）。

30

【0032】

受信したコマンドがlookupコマンドでない場合は、更にhitリプライであるかどうかを判断する（ステップS3）。hitリプライでもない場合は、その受信したコマンドに従ってその他の処理を行う（ステップS4）。一方、hitリプライを受信した場合、NATサーバ16は、マスカレードノードとして動作する自身のグローバルIPをhitリプライ中に付加し（ステップS5）、当該グローバルIPの付加されたhitリプライを他のノードに伝播する（ステップS6）。

40

【0033】

また、図3は、コマンド発行元ノード10の動作を示すフローチャートである。このフローチャートは、コマンド発行元ノード10が他のノードからhitリプライを受信した際の動作を示すものである。図3において、コマンド発行元ノード10は、受信したhitリプライ中に含まれている検索ヒットノード21のプライベートIPに基づいて、当該検索ヒットノード21にアクセスを試みる（ステップS11）。

【0034】

そして、アクセスのセッションが張れたかどうかを判断する（ステップS12）。プライ

50

プライベートネットワーク 20 の内部同士あるいは外部同士でアクセスするような場合には、セッションを張ることができる。したがって、例えば検索ヒットノードもコマンド発行元ノード 10 と同様にプライベートネットワーク 20 の外部にあるような場合には、コマンド発行元ノード 10 はそのアクセスに基づいて検索ヒットノードからリソースを取得する（ステップ S 14）。

【0035】

ただし、今の例では、検索ヒットノード 21 がプライベートネットワーク 20 の内部にあるので、プライベートネットワーク 20 の外部にあるコマンド発行元ノード 10 からその検索ヒットノード 21 に対してはアクセスのセッションを張ることができない。この場合、コマンド発行元ノード 10 は、hitリプライ中に含まれている NAT サーバ 16 のグローバル IP に基づいて、マスカレードノードへのアクセスに切り替えて検索ヒットノード 21 にアクセスし（ステップ S 13）、リソースを取得する（ステップ S 14）。 10

【0036】

以上詳しく説明したように、第 1 の実施形態によれば、hitリプライにマスカレードノードとしての NAT サーバのグローバル IP を付加して伝播するとともに、コマンド発行元ノードが検索ヒットノードにアクセスしてセッションを張れないときはマスカレードノードへのアクセスに切り替えて検索ヒットノードにアクセスするようにしたので、NAT サーバが設置されている場合でも、プライベートネットワークの外部から内部へと自由にアクセスすることができるようになる。

【0037】

（第 2 の実施形態） 20

次に、本発明の第 2 の実施形態を図面に基づいて説明する。

図 4 は、第 2 の実施形態によるネットワークの概略構成例を示す図である。本実施形態のネットワークは、ノードの集合 10 ～ 15、21 を含んで構成されている。

【0038】

図 4 の例において、ノード 21 はファイアウォール 40 の内部にあるものとする。また、その他のノード 10 ～ 15 はファイアウォール 40 の外部にあるものとする。本実施形態において、接続のセッションは、張れない場合には対処しない。しかし、接続セッションをファイアウォール 40 の内部または外部のどちらから張るかは問題でなく、張れる方向のみで接続セッションを開始して、トポロジを形成する。 30

【0039】

図 4 の例では、ファイアウォール 40 内のノード 21 から外部のノード 11、15 に対してセッションを開始することにより、これらの間に既に接続が確立している状態を示している。このような状態で、ノード 10 からリソース 30 を検索するための look up コマンドを発行した結果、ノード 11 を経由してファイアウォール 40 内のノード 21 に look up コマンドが伝播され、当該ノード 21 から逆の流れで hitリプライが返されてきたとする。

【0040】

hitリプライを受け取ったコマンド発行元ノード 10 は、通常の処理に従って、検索ヒットノード 21 に対してダイレクトにアクセスを試みる。しかし、検索ヒットノード 21 はファイアウォール 40 の内部に存在するので、コマンド発行元ノード 10 から検索ヒットノード 21 に対してはアクセスのセッションを張ることができない。 40

【0041】

この場合、コマンド発行元ノード 10 は、接続のセッションを通して、検索ヒットノード 21 に対して push-req コマンド（アクセス要求コマンド）を発行する。この push-req コマンドは、hitリプライが逆伝播された経路に従って、検索ヒットノード 21 に届けられる。push-req コマンドは、コマンド発行元ノード 10 の情報を含むパケットである。したがって、この push-req コマンドを受信した検索ヒットノード 21 では、コマンド発行元ノード 10 を知ることができる。

【0042】

そこで、`push-req` コマンドを受け取った検索ヒットノード 21 は、コマンド発行元ノード 10 に対してアクセスする。これは、通常のアクセス時と逆向きのセッションの張り方となる。ここでは、ファイアウォール 40 の内側から外側に向かうアクセスなので、問題なくセッションを張ることができる。コマンド発行元ノード 10 は、このとき張られたアクセスのセッションを通じて検索ヒットノード 21 にアクセスし、リソース 30 を取得する。

【0043】

図 5 は、図 4 に示したコマンド発行元ノード 10 の動作を示すフローチャートである。このフローチャートは、コマンド発行元ノード 10 が他のノードから `hit` リプライを受信した際の動作を示すものである。図 5 において、コマンド発行元ノード 10 は、受信した `hit` リプライ中に含まれているアクセスインタフェースの名前および検索ヒットノード 21 の情報に基づいて、検索ヒットノード 21 にアクセスを試みる（ステップ S21）。 10

【0044】

そして、アクセスのセッションが張れたかどうかを判断する（ステップ S22）。ファイアウォール 40 の外部同士あるいはファイアウォール 40 の内部から外部へのアクセスをするような場合には、セッションを張ることができる。その場合、コマンド発行元ノード 10 はそのアクセスに基づいて検索ヒットノードからリソースを取得する（ステップ S26）。

【0045】

ただし、図 4 のようにファイアウォール 40 の外部から内部の検索ヒットノード 21 にアクセスするような場合は、アクセスのセッションを張ることができない。この場合、コマンド発行元ノード 10 は、`push-req` コマンドを発行する（ステップ S23）。その後、その `push-req` コマンドに従って検索ヒットノード 21 からアクセスが行われたかどうかを判断し（ステップ S24）、行われた場合には、そのアクセスのセッションを通じて検索ヒットノード 21 にアクセスして（ステップ S25）、リソース 30 を取得する（ステップ S26）。 20

【0046】

図 6 は、第 2 の実施形態によるネットワークの別の構成例を示す図である。図 6 に示す例では、検索ヒットノード 21 がファイアウォール 40 の内部にあるだけでなく、コマンド発行元ノード 10 も別のファイアウォール 41 の内部に含まれている。このような場合に対応するために、アクセスの仲介を行うためのゲートウェイノード（GW ノード）50 を各ファイアウォール 40、41 の外部に用意する。ゲートウェイノード 50 は、コマンド発行元ノード 10 および検索ヒットノード 21 の両方からセッションを張れる必要がある。 30

【0047】

この図 6 の例においても、ノード 10 からリソース 30 を検索するための `lookup` コマンドを発行した結果、ノード 11 を経由してファイアウォール 40 内のノード 21 に `lookup` コマンドが伝播され、当該ノード 21 から逆の流れで `hit` リプライが返されてきたとする。

【0048】

`hit` リプライを受け取ったコマンド発行元ノード 10 は、通常の処理に従って、検索ヒットノード 21 に対してダイレクトにアクセスを試みる。しかし、検索ヒットノード 21 はファイアウォール 40 の内部に存在するので、コマンド発行元ノード 10 から検索ヒットノード 21 に対してはアクセスのセッションを張ることができない。 40

【0049】

この場合、コマンド発行元ノード 10 は、`hit` リプライが逆伝播された接続経路に沿って、検索ヒットノード 21 に対して `push-req` コマンドを発行する。`push-req` コマンドを受け取った検索ヒットノード 21 は、コマンド発行元ノード 10 に対してアクセスを試みる。これは、通常のアクセス時と逆向きのセッションの張り方となる。

【0050】

先に示した図4の例では、この時点でアクセスのセッションを張ることができた。しかし、ここでは、コマンド発行元ノード10もファイアウォール41の内部に存在するので、検索ヒットノード21からコマンド発行元ノード10に対してもアクセスのセッションを張ることができない。

【0051】

この場合、コマンド発行元ノード10は、接続のセッションを通して、検索ヒットノード21に対してg w - r e q コマンド（ゲートウェイアクセス要求コマンド）を発行する。このg w - r e q コマンドは、h i t リプライが逆伝播された経路に従って、検索ヒットノード21に届けられる。g w - r e q コマンドは、ゲートウェイノード50の情報を含むパケットである。したがって、このg w - r e q コマンドを発行したコマンド発行元ノード10およびこれを受信した検索ヒットノード21の双方は、ゲートウェイノード50を知ることができる。

10

【0052】

そこで、コマンド発行元ノード10および検索ヒットノード21は、ゲートウェイノード50に対してアクセスする。これらは共に、ファイアウォール40の内側から外側に向かうアクセスなので、問題なくセッションを張ることができる。ゲートウェイノード50は、内部的に2つのセッションを結び付けて、アクセスのセッションを仲介する。コマンド発行元ノード10は、このとき張られたアクセスセッションを通じて検索ヒットノード21にアクセスし、リソース30を取得する。

【0053】

図7は、図6に示したコマンド発行元ノード10の動作を示すフローチャートである。このフローチャートは、コマンド発行元ノード10が他のノードからh i t リプライを受信した際の動作を示すものである。図7において、コマンド発行元ノード10は、受信したh i t リプライ中に含まれているアクセスインタフェースの名前および検索ヒットノード21の情報をもとに、検索ヒットノード21にアクセスを試みる（ステップS31）。

20

【0054】

そして、アクセスのセッションが張れたかどうかを判断する（ステップS32）。ここでアクセスのセッションを張ることができた場合、コマンド発行元ノード10はそのアクセスに基づいて検索ヒットノードからリソースを取得する（ステップS38）。

【0055】

一方、図6のようにファイアウォール40の外部から内部の検索ヒットノード21にアクセスするような場合は、アクセスのセッションを張ることができない。この場合、コマンド発行元ノード10は、p u s h - r e q コマンドを発行する（ステップS33）。その後、そのp u s h - r e q コマンドに従って検索ヒットノード21からアクセスが行われたかどうかを判断し（ステップS34）、行われた場合には、そのアクセスのセッションを通じて検索ヒットノード21にアクセスして（ステップS35）、リソース30を取得する（ステップS38）。

30

【0056】

しかし、図6の例では検索ヒットノード21からコマンド発行元ノード10に対してもアクセスのセッションを張ることができない。この場合、コマンド発行元ノード10は、検索ヒットノード21に対してg w - r e q コマンドを発行した後（ステップS36）、ゲートウェイノード50にアクセスする（ステップS37）。検索ヒットノード21にg w - r e q コマンドを発行することによって、検索ヒットノード21からもゲートウェイノード50へのアクセスが行われるので、コマンド発行元ノード10はこれらのアクセスセッションを通じて検索ヒットノード21にアクセスし、リソース30を取得する（ステップS38）。

40

【0057】

図8は、図6に示した検索ヒットノード21の動作を示すフローチャートである。このフローチャートは、検索ヒットノード21が他のノードにh i t リプライを発行した後の動作を示すものである。図8において、検索ヒットノード21は、p u s h - r e q コマ

50

ドを受信したかどうかを判断する（ステップS41）。push-reqコマンドを受信していない場合は、コマンド発行元ノード10から検索ヒットノード21に対するアクセスのセッションがうまく張られたということなので、何もせずに処理を終了する。

【0058】

一方、push-reqコマンドを受信した場合は、その受信したpush-reqコマンド中に含まれているコマンド発行元ノード10の情報をもとに、当該コマンド発行元ノード10にアクセスを試みる（ステップS42）。そして、アクセスのセッションが張れたかどうかを判断する（ステップS43）。ここでアクセスのセッションを張ることができた場合は、何もせずに処理を終了する。

【0059】

検索ヒットノード21からコマンド発行元ノード10に対してアクセスのセッションを張ることができなかった場合、検索ヒットノード21はgwr-reqコマンドの受信待ちの状態になる（ステップS44）。gwr-reqコマンドを受信した場合は、その受信したgwr-reqコマンド中に含まれているゲートウェイノード50の情報をもとに、当該ゲートウェイノード50にアクセスして（ステップS45）処理を終了する。

【0060】

以上詳しく説明したように、第2の実施形態によれば、ファイアウォール内のリソースに外部からアクセスしようとする場合に、所定のコマンドを発行することによってファイアウォールの内側から外側に向かってアクセスのセッションを張るようにしたので、セキュリティ対策のためにファイアウォールを設置した場合でも、そのファイアウォールの外部から内部のリソースへと自由にアクセスすることができるようになる。

【0061】

なお、このようにファイアウォールの内向きに自由にアクセスできるようになると、不正な第三者がグループのメンバに成りすましてファイアウォール内に侵入することもあり得る。本実施形態では、このような場合にも機密情報が漏れないように、転送するデータやファイル等のリソースを暗号化する。また、ユーザ認証も利用する。なお、暗号化の方式は特に限定しないが、例えばPKI（公開鍵暗号方式）を利用することが可能である。

【0062】

本実施形態では、ユーザログイン時に認証のタイプを指定することができるようにしている。認証には、単純なパスワード認証から複雑なSSL（Secure Sockets Layer）認証まで用意されている。パスワード認証は、各ノード上で実行される。SSL認証は、各ノードが接続時に提出する証明書をベースにして行われる。

【0063】

図9は、ユーザ情報を告知する際の動作を説明するための図である。図9に示すように、ユーザノード10は、ネットワークへのログイン後および新たな接続の開始時に、接続セッションを利用してユーザ情報を告知する。このユーザ情報は、ユーザID、表示名、説明、ユーザ認証の証明書（公開鍵）を含む。ユーザノード10から告知されたユーザ情報のパケットは、他のノード11～19間で伝播される。

【0064】

ユーザノード10から伝播されたユーザ情報は、各ノード11～19のローカルストレージが備える共通ユーザリスト61、62、・・・に各々キャッシュ記憶される。ユーザ認証やデータの暗号化あるいは復号化を行うときは、この共通ユーザリスト61、62、・・・に記憶されたユーザ情報を取得して利用する。

【0065】

図10は、SSLベースのユーザ認証を行う際の動作を説明するための図である。SSL認証を行う場合、認証する側には、認証局の証明書が必要となる。そのためノードは、所定の属性ファイルと認証局の証明書とをセットで配布する。図9で説明したように、ノードにユーザがログインすると、ユーザノード10は、その接続先にユーザの証明書を提出する。ユーザの証明書を受けたノードは、認証局の証明書で当該ユーザ証明書を認証する。証明書の認証後、ユーザの秘密鍵の本人確認を行い、これに認められた場合にログイン

10

20

30

40

50

を許可する。

【0066】

ユーザ認証時に提出された証明書は、ユーザ情報の告知として他のノードに伝播される。各ノードは、受け取ったユーザ証明書をローカルストレージにキャッシュする。リソースをSSLベースで暗号化するときや、リソースの署名を確認するときなどは、ユーザ証明書内の公開鍵を使用する。

【0067】

このように、本実施形態では、ネットワークへのログイン時などにユーザ情報の告知を行うようにし、そのユーザ情報の中にユーザ証明書（公開鍵を含む）を含ませるようにしたので、各ノードに対して公開鍵を容易に配布することができる。逆に言えば、各ノードで公開鍵を入手するのが非常に容易であり、P2Pネットワークの中でユーザ認証および暗号化を容易に行うことができる。

【0068】

以上に説明した本実施形態によるネットワークシステムの機能は、実際にはコンピュータのCPUあるいはMPU、RAM、ROMなどで構成され、RAMやROMに記憶されたプログラムが動作することによって実現できる。したがって、コンピュータが上記の機能を果たすように動作させるプログラムを例えばCD-ROMのような記録媒体に記録し、コンピュータに読み込ませることによって実現できるものである。

【0069】

上記プログラムを記録する記録媒体としては、CD-ROM以外に、フレキシブルディスク、ハードディスク、磁気テープ、光ディスク、光磁気ディスク、DVD、不揮発性メモ리카ード等を用いることができる。また、上記プログラムをインターネット等のネットワークを介してコンピュータにダウンロードすることによっても実現できる。

【0070】

また、コンピュータが供給されたプログラムを実行することにより上述の実施形態の機能が実現されるだけでなく、そのプログラムがコンピュータにおいて稼働しているOS（オペレーティングシステム）あるいは他のアプリケーションソフト等と共同して上述の実施形態の機能が実現される場合や、供給されたプログラムの処理の全てあるいは一部がコンピュータの機能拡張ボードや機能拡張ユニットにより行われて上述の実施形態の機能が実現される場合も、かかるプログラムは本実施形態に含まれる。

【0071】

なお、上記に説明した各実施形態は、本発明を実施するにあたっての具体化の一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【0072】

【発明の効果】

本発明は上述したように、グローバルアドレスとプライベートアドレスとの付け替えを行うゲートウェイノードが検索ヒット応答を受け取ったときに、検索ヒットノードの情報にゲートウェイノードの情報を加えて伝播するようにし、コマンド発行元ノードが検索ヒット応答を受け取ったときは、当該検索ヒット応答中に含まれる検索ヒットノードの情報およびゲートウェイノードの情報に基づき検索ヒットノードもしくはゲートウェイノードにアクセスするようにしている。これにより、ゲートウェイノードが存在する場合でも、プライベートネットワークの外部から内部あるいはその逆へと自由にアクセスしてリソースを取得することができるようになる。

【0073】

本発明の他の特徴によれば、コマンド発行元ノードが検索ヒットノードにアクセスできないときに、接続している近接ノード群を介してアクセス要求コマンドを検索ヒットノードに伝播するとともに、これを受け取った検索ヒットノードがコマンド発行元ノードにアクセスを実行するようにしている。これにより、ファイアウォールの外側から内側に向かっ

10

20

30

40

50

てアクセスできない場合でも、上記アクセス要求コマンドを発行することによってファイアウォールの内側から外側に向かってアクセスを確立することができ、そのセッションを利用してファイアウォールの外部から内部のリソースへと自由にアクセスすることができるようになる。

【0074】

また、本発明の他の特徴によれば、コマンド発行元ノードがアクセス要求コマンドを発行したにもかかわらず検索ヒットノードからのアクセスが確立されないときに、所定のゲートウェイノードにアクセスするとともに、当該ゲートウェイノードへのアクセス要求コマンドを近接ノード群を介して検索ヒットノードに伝播し、これを受け取った検索ヒットノードがゲートウェイノードにアクセスを実行するようにしている。これにより、コマンド発行元ノードと検索ヒットノードとの双方がファイアウォールの中にある場合であっても、それぞれのファイアウォールの内側から外側のゲートウェイノードに向かってアクセスを確立することができ、それらのセッションを利用してファイアウォールの外部から内部のリソースへと自由にアクセスすることができるようになる。

10

【図面の簡単な説明】

【図1】第1の実施形態によるネットワークの概略構成例を示す図である。

【図2】第1の実施形態によるNATサーバの動作を示すフローチャートである。

【図3】第1の実施形態によるコマンド発行元ノードの動作を示すフローチャートである。

【図4】第2の実施形態によるネットワークの概略構成例を示す図である。

20

【図5】図4に示したコマンド発行元ノードの動作を示すフローチャートである。

【図6】第2の実施形態によるネットワークの別の構成例を示す図である。

【図7】図6に示したコマンド発行元ノードの動作を示すフローチャートである。

【図8】図6に示した検索ヒットノードの動作を示すフローチャートである。

【図9】ユーザ情報の告知動作を示すフローチャートである。

【図10】SSLベースのユーザ認証を行う際の動作を説明するための図である。

【図11】P2Pアーキテクチャを利用して所望のリソースを検索および取得する際の手順を示す図である。

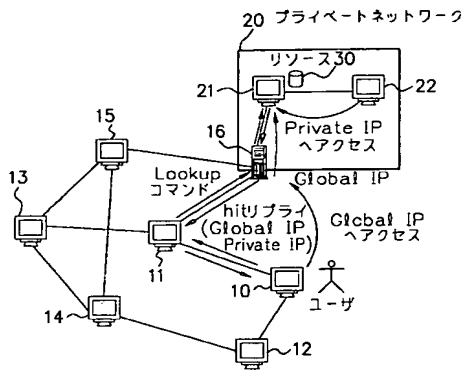
【符号の説明】

- 10～15 ノード
- 16 マスカレードノード（NATサーバ）
- 20 プライベートネットワーク
- 21～22 ノード
- 30 リソース
- 40, 41 ファイアウォール
- 50 ゲートウェイノード
- 61, 62 共通ユーザリスト

30

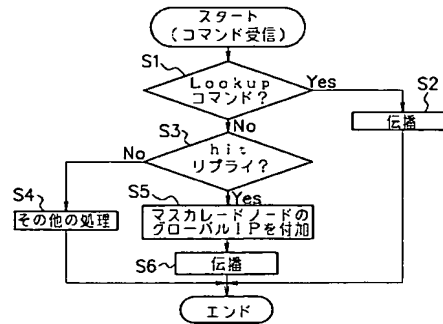
【図 1】

第1の実施形態によるネットワーク



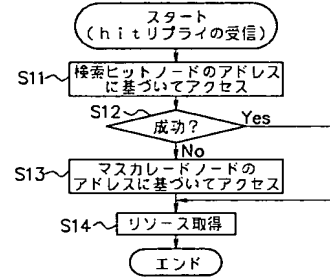
【図 2】

NATサーバの動作



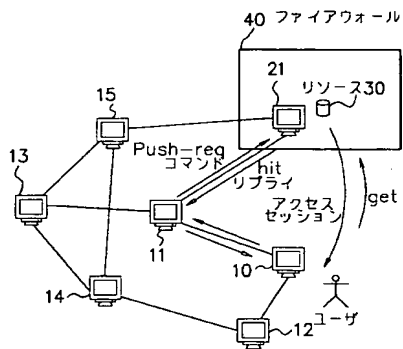
【図 3】

第1の実施形態によるコマンド発行元ノードの動作



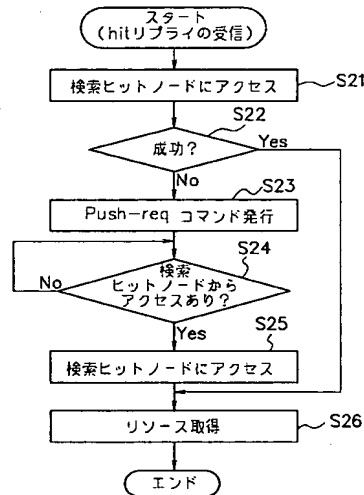
【図 4】

第2の実施形態によるネットワーク



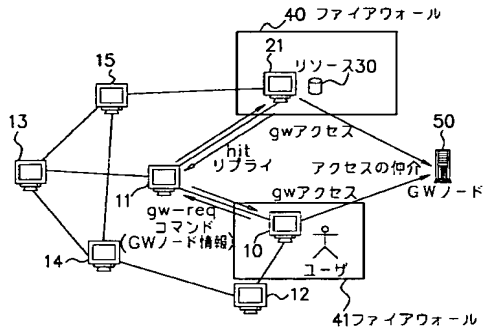
【図 5】

第2の実施形態によるコマンド発行元ノードの動作



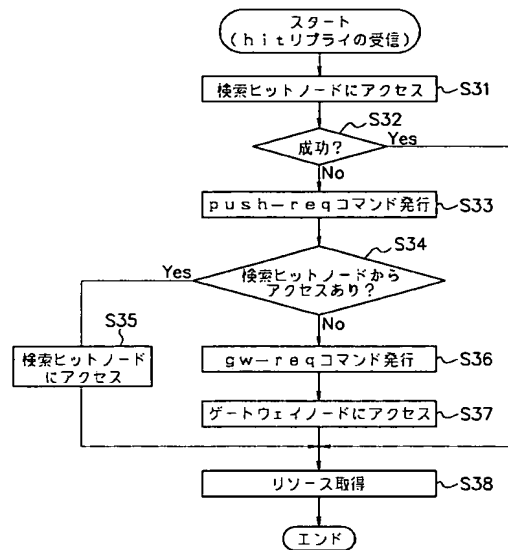
【図 6】

第2の実施形態によるネットワークの別の例



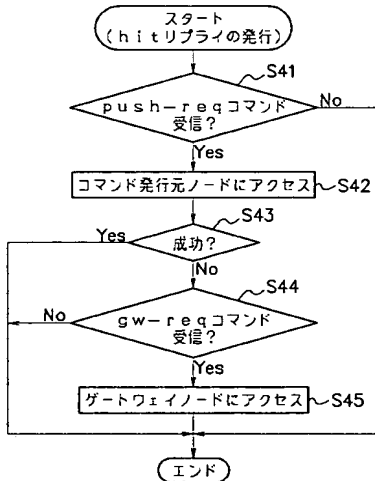
【図 7】

第2の実施形態によるコマンド発行元ノードの他の動作



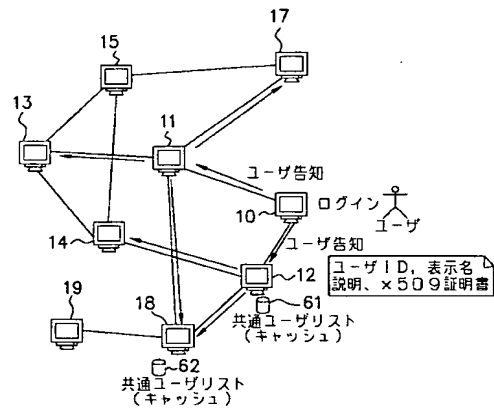
【図 8】

第2の実施形態による検索ヒットノードの動作



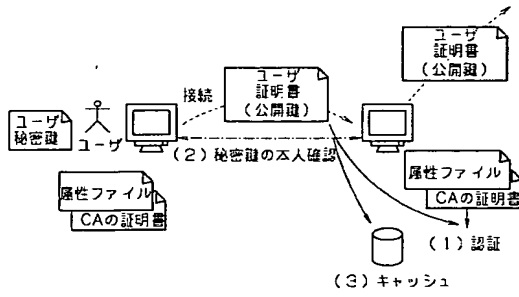
【図 9】

ユーザ情報の告知動作

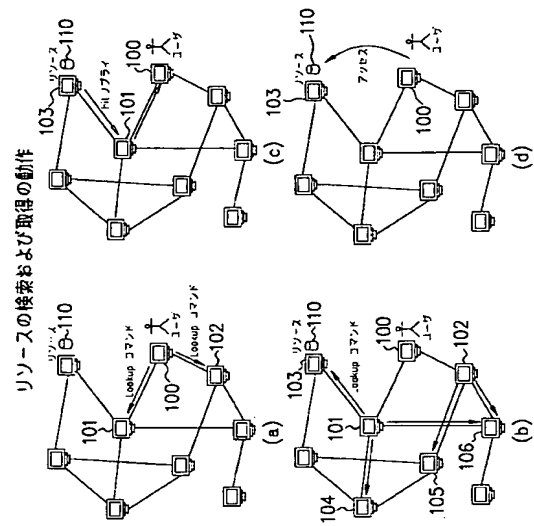


【図 10】

ユーザ認証の動作



【図 11】



フロントページの続き

(72)発明者 岩田 真一

東京都八王子市大和田町3丁目14番地16号

Fターム(参考) 5B085 BA06

5K030 GA14 HA08 HD09 KA05 KA15 LD19 MD10

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record.**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☒ **FADED TEXT OR DRAWING**

☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.